



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/716,336	11/18/2003	Nicholas Stamos	3602.1000-003	5223

21005 7590 08/08/2007
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER

LEMMÄ, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

MAIL DATE	DELIVERY MODE
-----------	---------------

08/08/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/716,336

Applicant(s)

STAMOS ET AL.

Examiner

Samson B. Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 May 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 06/28/07.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application
- ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on May 16, 2007.

Claims 1, 2, 6, 8, 10, 11, 14-17 and 21 are amended and claim 1-22 are pending/**examined**.

Response to Arguments

2. Applicant's remarks/arguments filed on May 16, 2007 have been fully considered but they are not persuasive.

Applicant amended independent claim 1 and 17 and argued that the limitation added to the respective independent claims are not disclosed by the reference on the record, namely Belfiore.

In order to support his argument applicant wrote the following.

"Belfiore does not teach or suggest "a sensor to sense atomic level events, the sensor located within an operating system kernel within a user client device" as now claimed in independent Claim 1. While Belfiore discloses event sources that generate atomic events that are then provided to an event composition mechanism, Belfiore does not disclose that the event sources capture or sense the atomic events. Moreover, Belfiore does not disclose that the event sources are located within an operating system kernel within a user client device. (See Belfiore col. 20, lines 46-60)"

Examiner disagrees with the above argument.

Examiner would like to point out that all limitation recited in the amended independent claims are still disclosed by the reference on the record.

In order to show how each and every limitation of the amended independent claims are disclosed by the reference on the record the examiner would show the following.

Art Unit: 2132

For instance regarding the amended independent claims 1 and 17, the reference on the record namely Belfiore discloses a system for journaling activity in a data processing system comprising:

- **A sensor for to sense or capture atomic level events;** *[column 20, lines 57-58, figure 5, ref. Num "606" see "atomic events provided by event sources 602"/As shown on figure 5, ref. Num "606" the atomic events are captured)* **the sensor located within an operating system kernel within a user client device;** *Column 28, lines 1-6 and column 22, lines 46-56] [For instance on column 28, lines 1-6 the following has been disclosed. "In one embodiment, the HTTP client is implemented in kernel mode. Reasons for implementation in kernel mode include 1) performance; 2) communication with kernel components; and 3) listener/talker integration. The benefits of listener/talker integration include performance optimizations and shared implementation." Furthermore on column 22, lines 46-56 the following has been disclosed. The event system includes a highly optimized publication and subscription service driven by model-based subscription registrations. The events system allows for flexibility and choice of the service to publish events, such as, by way of example, kernel events (e.g. WDM drivers events) that utilize a kernel driver programming model, non-COM APIs for publishing events (e.g. security audit events, a directory, a service control manager) that utilize a low-level operating system service programming model, classic COM interfaces for normal applications, and high-level COM+ classes that utilize native COM+ programming model.) and*

- **An aggregator, to accept or for accepting multiple atomic level events and to generate an aggregate event based on a predetermined sequence of atomic level events.** *[column 21, lines 4-12 and column 20, lines 57-67] (Event composition 608 **aggregates, filters, and transforms lower-level***

Art Unit: 2132

events (atomic events 606) which meets the limitation of “multiple atomic level events” into higher-level events 612, which meets the limitation of a journal/aggregate event. And, at times, maps the events directly into actions, such as world action 614. The actions include real-world actions 614 and information-gathering actions 616 that serve to gather new events via actively polling or listening. **Event composition 608 provides methods for combining events and data, whether the events are observed in close temporal proximity or at widely different times.** On column 20, lines 57-67, the following has also been disclosed, **“The event component 155 transforms fundamental or atomic events 606 provided by event sources 602 into progressively higher-level events/predetermined sequence of atomic level; through an event composition mechanism 608.** The process of event composition is the construction of new events or actions from a set of observed events and/or stored event data. Event composition may be driven by rules, filters, and by more advanced pattern recognizers spanning a spectrum of sophistication all the way up to rich inferential machinery. Thus, event composition adapts the set of available atomic events 606 into observations 610 that are appropriately matched to the informational requirements of software components, providing them with information at the right level of abstraction to make good decisions.)

Therefore all limitations recited in the independent claims are undoubtedly disclosed by the reference/s on the record and the rejection is maintained until the applicant amends at least the independent claims and successfully overcome the rejection without introducing new matters.

Claim Rejections - 35 USC § 102

Art Unit: 2132

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1-22** are rejected under 35 U.S.C. 102(e) as being anticipated by **Belfiore et al.** (hereinafter referred as **Belfiore**)(U.S. Patent No. 6,990,513 B2) (filed on Jun 22, 2001)
5. **As per claims 1 and 16-17 Belfiore discloses a system for journaling activity in a data processing system comprising:**

- **A sensor for to sense or capture atomic level events;** [column 20, lines 57-58, figure 5, ref. Num "606" see "atomic events provided by event sources 602"/As shown on figure 5, ref. Num "606" the atomic events are captured) **the sensor located within an operating system kernel within a user client device;** Column 28, lines 1-6 and column 22, lines 46-56] [For instance on column 28, lines 1-6 the following has been disclosed. "In one embodiment, the HTTP client is implemented in kernel mode. Reasons for implementation in kernel mode include 1) performance; 2) communication with kernel components; and 3) listener/talker integration. The benefits of listener/talker integration include performance optimizations and shared implementation." Furthermore on column 22, lines 46-56 the following has been disclosed. The event system includes a highly optimized publication and subscription service driven by model-based subscription registrations. The events system allows for flexibility and choice of the service to publish events, such as,

Art Unit: 2132

by way of example, kernel events (e.g. WDM drivers events) that utilize a kernel driver programming model, non-COM APIs for publishing events (e.g. security audit events, a directory, a service control manager) that utilize a low-level operating system service programming model, classic COM interfaces for normal applications, and high-level COM+ classes that utilize native COM+ programming model.) and

- **An aggregator, to accept or for accepting multiple atomic level events and to generate an aggregate event based on a predetermined sequence of atomic level events.** [column 21, lines 4-12 and column 20, lines 57-67] (Event composition 608 **aggregates, filters, and transforms lower-level events (atomic events 606) which meets the limitation of “multiple atomic level events”** into higher-level events 612, which meets the limitation of a journal/aggregate event. And, at times, maps the events directly into actions, such as world action 614. The actions include real-world actions 614 and information-gathering actions 616 that serve to gather new events via actively polling or listening. **Event composition 608 provides methods for combining events and data, whether the events are observed in close temporal proximity or at widely different times.** On column 20, lines 57-67, the following has also been disclosed, **“The event component 155 transforms fundamental or atomic events 606 provided by event sources 602 into progressively higher-level events/predetermined sequence of atomic level; through an event composition mechanism 608.** The process of event composition is the construction of new events or actions from a set of observed events and/or stored event data. Event composition may be driven by rules, filters, and by more advanced pattern recognizers spanning a spectrum of sophistication all the way up to rich inferential machinery. Thus, event composition adapts the set of available atomic events 606 into observations 610 that are appropriately matched to the informational

Art Unit: 2132

requirements of software components, providing them with information at the right level of abstraction to make good decisions.)

6. As per claims 2-3 Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein, the aggregate events are associated with a particular executing process/with a particular user.

[column 34-45 and column 21, lines 4-12 and column 20, lines 57-67] *(The event component 155 of the present invention transparently facilitates the distributed communication of events between any software component that publishes or generates events ("event source") and any software component that subscribes to or receives event notifications ("event sink"). In this description and in the claims, an event is an observation about one or more states such as, for example, the status of system components, **the activity of a user.**)*

7. As per claims 4 and 18 Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system additionally comprising: a filter for filtering atomic level events with an approved event list.

[Column 21, lines 4-19 and column 20, lines 62-column 21, lines 3 and column 22, lines 63-64] *(Event composition 608 aggregates, filters, and transforms lower-level events (atomic events 606) into higher-level events 612 and, at times, maps the events directly into actions, such as world action 614. and on column lines it has been disclosed that Event composition may be driven by rules, filters, and by more advanced pattern recognizers spanning a spectrum of sophistication all the way up to rich inferential machinery. Thus, event composition adapts the set of available atomic events 606 into observations 610 that are appropriately matched to **the informational requirements of software components/ such requirements meets the limitation of approved event list**, providing them with information at the right level of abstraction to make good decisions.)*

Art Unit: 2132

8. **As per claims 5-6 and 19** Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein the approved event list includes a list of approved file identifiers/hash code. [Figure 5, ref. Num 610/612 and 622, column 21, lines 3-35] (As shown on figure 5, High level events shown as 612 which meets the limitation of approved event list is stored in event store as shown on figure 5, 622 inferences are performed. Such events should have some kinds of identifier when they are stored and hashing a value for the sake of utilizing the space requirement is something which is also included in storing the list of approved file identifiers /high level events 612)

9. **As per claims 7 and 20** Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system, wherein the sensor is located within a client agent and the aggregator is located within a server. [Column 21, lines 36-44]

10. **As per claims 8 and 21** Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system additionally comprising: a coalescer to coalesce atomic multiple events output by the sensor into a single event prior to inputting them to the aggregator. [Figure 5, ref. Num "606"]

11. **As per claims 9-10 and 22** Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein a bundle of coalesced events is created prior to their transmission between the agent and the server. [Figure 5, ref. Num "608"/event composition meets the limitation of a bundle of coalesced events]

12. **As per claim 11** Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein a an aggregate

Art Unit: 2132

/journal event is detected as a suspect action with a data file. [column 23, lines 64-column 24, lines 22 and column 21, lines 4-12 and column 20, lines 57-67]

13. **As per claim 12 Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein an event is attributable to a known user, thread and/or application as identified at a known time. [figure 5, see "Time"]

14. **As per claim 13 Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein the coalescer reports an event after a time out period with no activity. [column 24, lines 21-22, "notify me if there is no mouse movement and no key is pressed in 5 minutes"]

15. **As per claims 14-15 Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein aggregate events are used to control security of the data processing system. [column 21, lines 50-53 and column 23, lines 64-column 24, lines 22 and column 21, lines 4-12 and column 20, lines 57-67]

Conclusion

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the

Art Unit: 2132

advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

08/01/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100